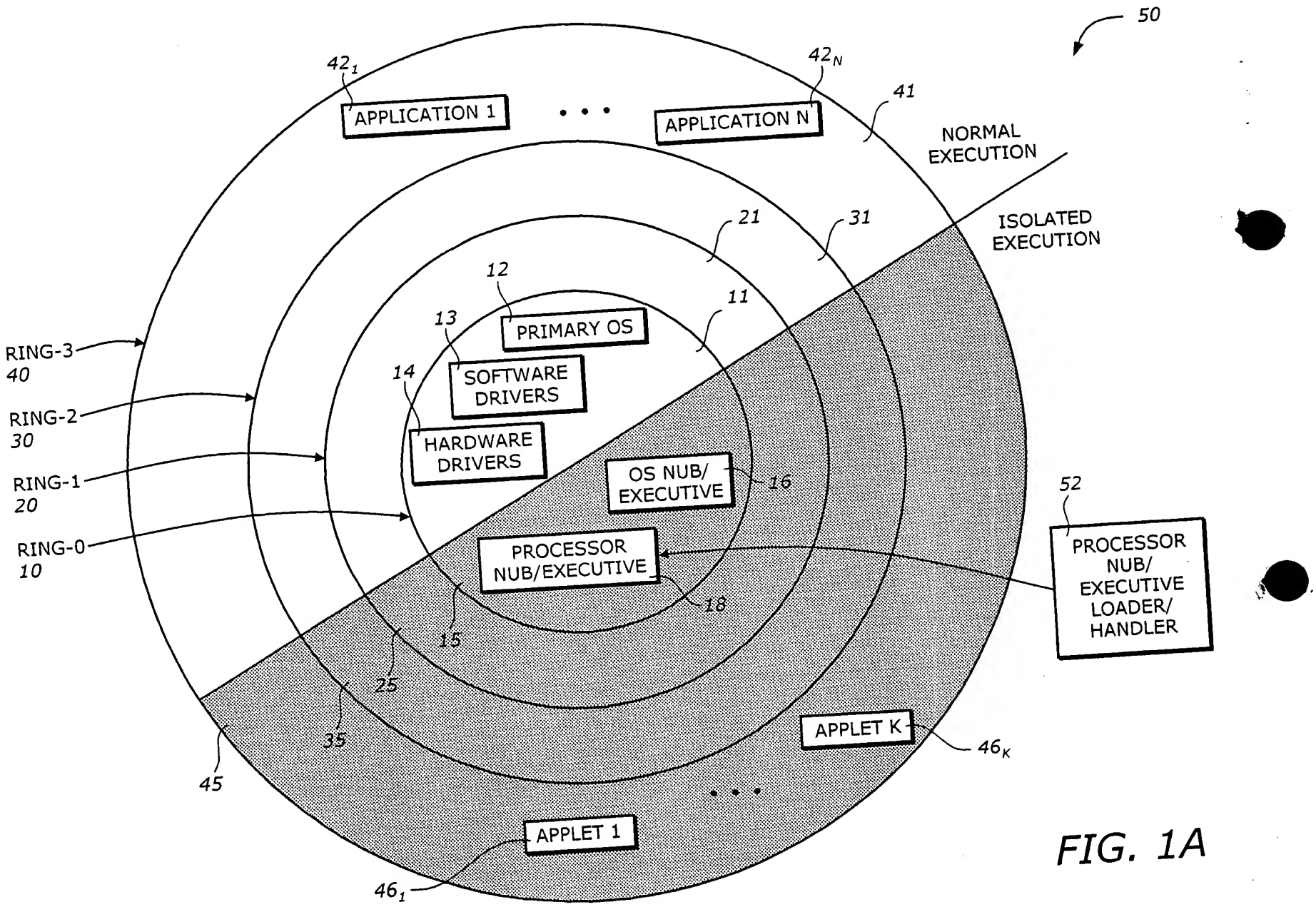
50
42_1
APPLICATION 1
42_N
APPLICATION N
41
NORMAL EXECUTION
ISOLATED EXECUTION
21
31
12
11
13
PRIMARY OS
SOFTWARE DRIVERS
14
HARDWARE DRIVERS
RING-3
40
RING-2
30
RING-1
20
RING-0
10
OS NUB/ EXECUTIVE
16
52
PROCESSOR NUB/EXECUTIVE
18
PROCESSOR NUB/ EXECUTIVE LOADER/ HANDLER
15
25
35
45
APPLET K
46_K
APPLET 1
46_1

FIG. 1A

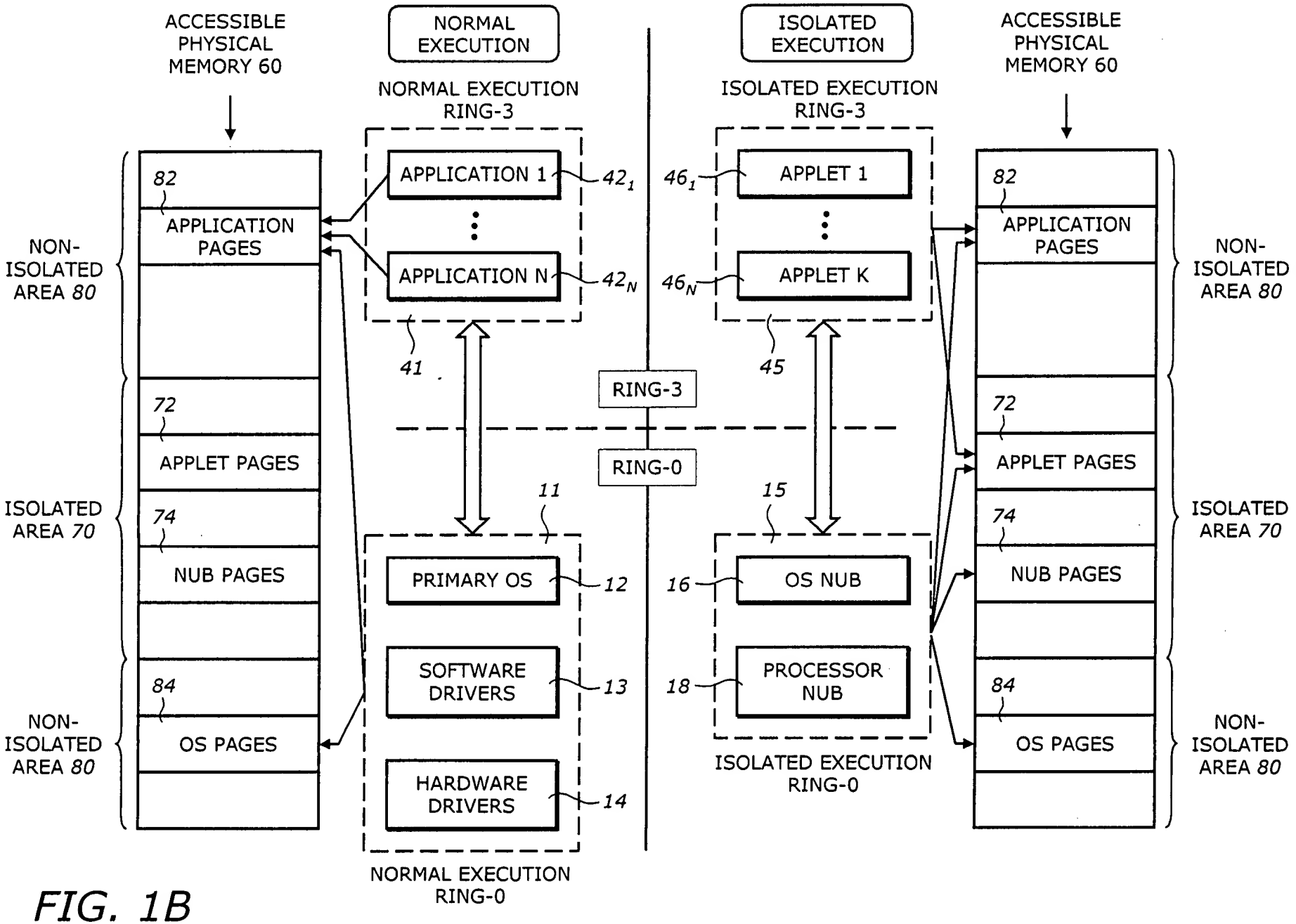
ACCESSIBLE PHYSICAL MEMORY 60
NORMAL EXECUTION
ISOLATED EXECUTION
ACCESSIBLE PHYSICAL MEMORY 60
NORMAL EXECUTION RING-3
ISOLATED EXECUTION RING-3
82
APPLICATION PAGES
APPLICATION 1
42₁
APPLICATION N
42N
46₁
APPLET 1
46N
APPLET K
NON-ISOLATED AREA 80
41
45
RING-3
RING-0
72
APPLET PAGES
11
15
ISOLATED AREA 70
74
NUB PAGES
PRIMARY OS
12
16
OS NUB
SOFTWARE DRIVERS
13
18
PROCESSOR NUB
84
OS PAGES
HARDWARE DRIVERS
14
NON-ISOLATED AREA 80
NORMAL EXECUTION RING-0
ISOLATED EXECUTION RING-0

FIG. 1B

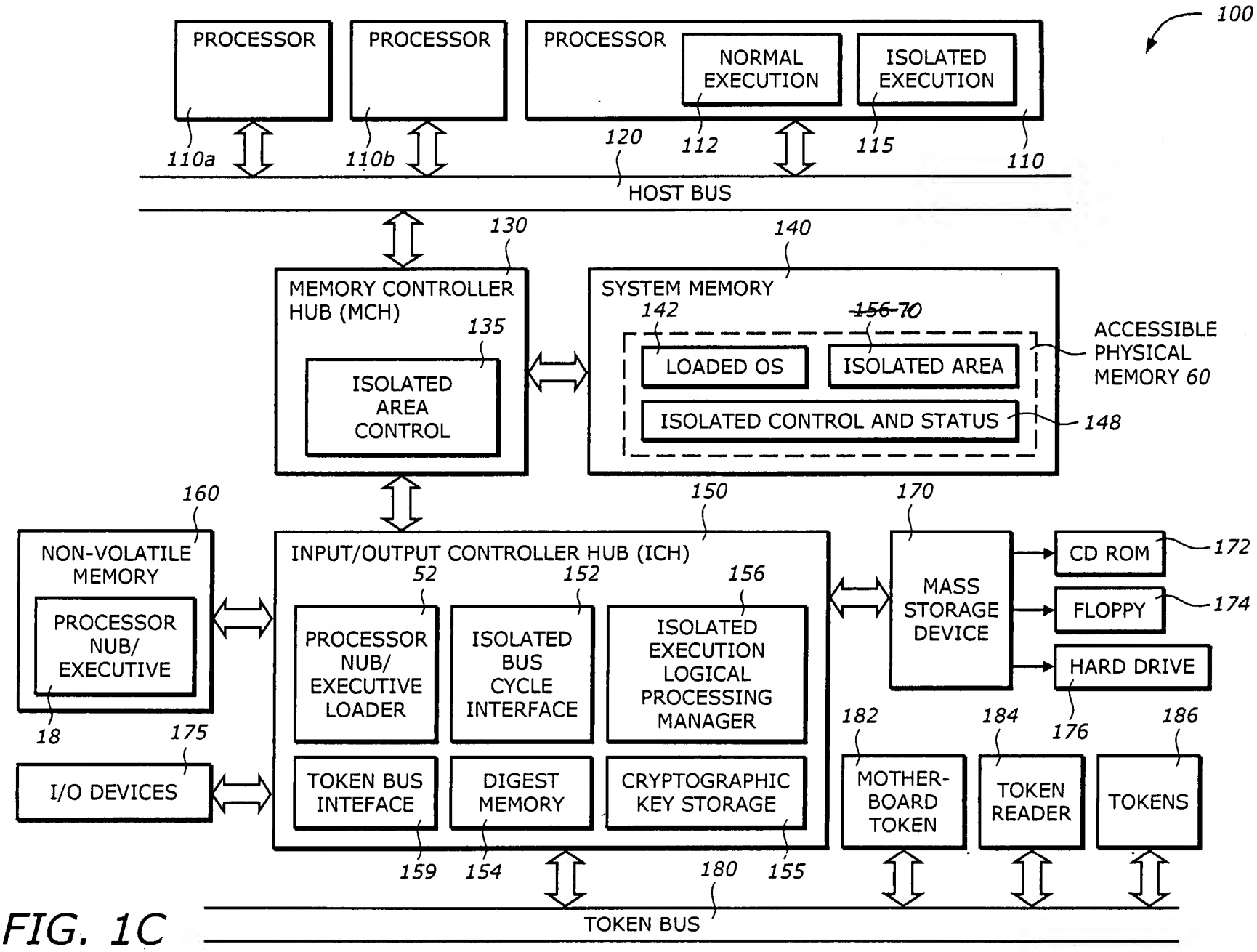
100
PROCESSOR
PROCESSOR
PROCESSOR
NORMAL EXECUTION
ISOLATED EXECUTION
110a
110b
120
112
115
110
HOST BUS
130
140
MEMORY CONTROLLER HUB (MCH)
135
ISOLATED AREA CONTROL
SYSTEM MEMORY
142
156-70
LOADED OS
ISOLATED AREA
ISOLATED CONTROL AND STATUS
148
ACCESSIBLE PHYSICAL MEMORY 60
160
150
170
NON-VOLATILE MEMORY
PROCESSOR NUB/ EXECUTIVE
18
175
INPUT/OUTPUT CONTROLLER HUB (ICH)
52
152
156
PROCESSOR NUB/ EXECUTIVE LOADER
ISOLATED BUS CYCLE INTERFACE
ISOLATED EXECUTION LOGICAL PROCESSING MANAGER
MASS STORAGE DEVICE
CD ROM
172
FLOPPY
174
HARD DRIVE
176
I/O DEVICES
TOKEN BUS INTEFACE
DIGEST MEMORY
CRYPTOGRAPHIC KEY STORAGE
182
184
186
MOTHER-BOARD TOKEN
TOKEN READER
TOKENS
159
154
180
155
TOKEN BUS

FIG. 1C

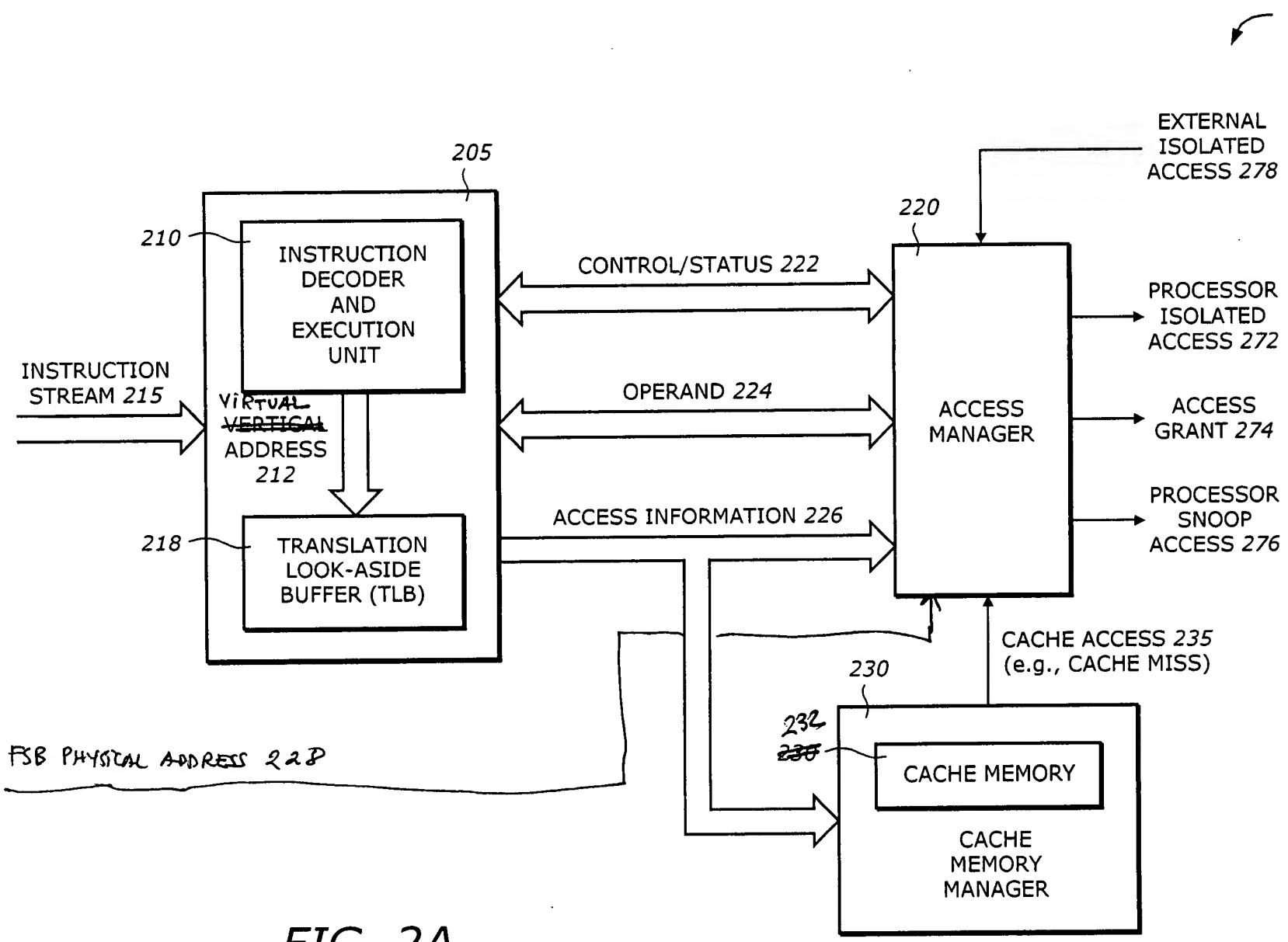
115
205
210
INSTRUCTION DECODER AND EXECUTION UNIT
INSTRUCTION STREAM 215
VIRTUAL ~~VERTICAL~~ ADDRESS 212
218
TRANSLATION LOOK-ASIDE BUFFER (TLB)
CONTROL/STATUS 222
OPERAND 224
ACCESS INFORMATION 226
220
ACCESS MANAGER
EXTERNAL ISOLATED ACCESS 278
PROCESSOR ISOLATED ACCESS 272
ACCESS GRANT 274
PROCESSOR SNOOP ACCESS 276
CACHE ACCESS 235 (e.g., CACHE MISS)
230
232
~~235~~
CACHE MEMORY
CACHE MEMORY MANAGER
FSB PHYSICAL ADDRESS 228

FIG. 2A

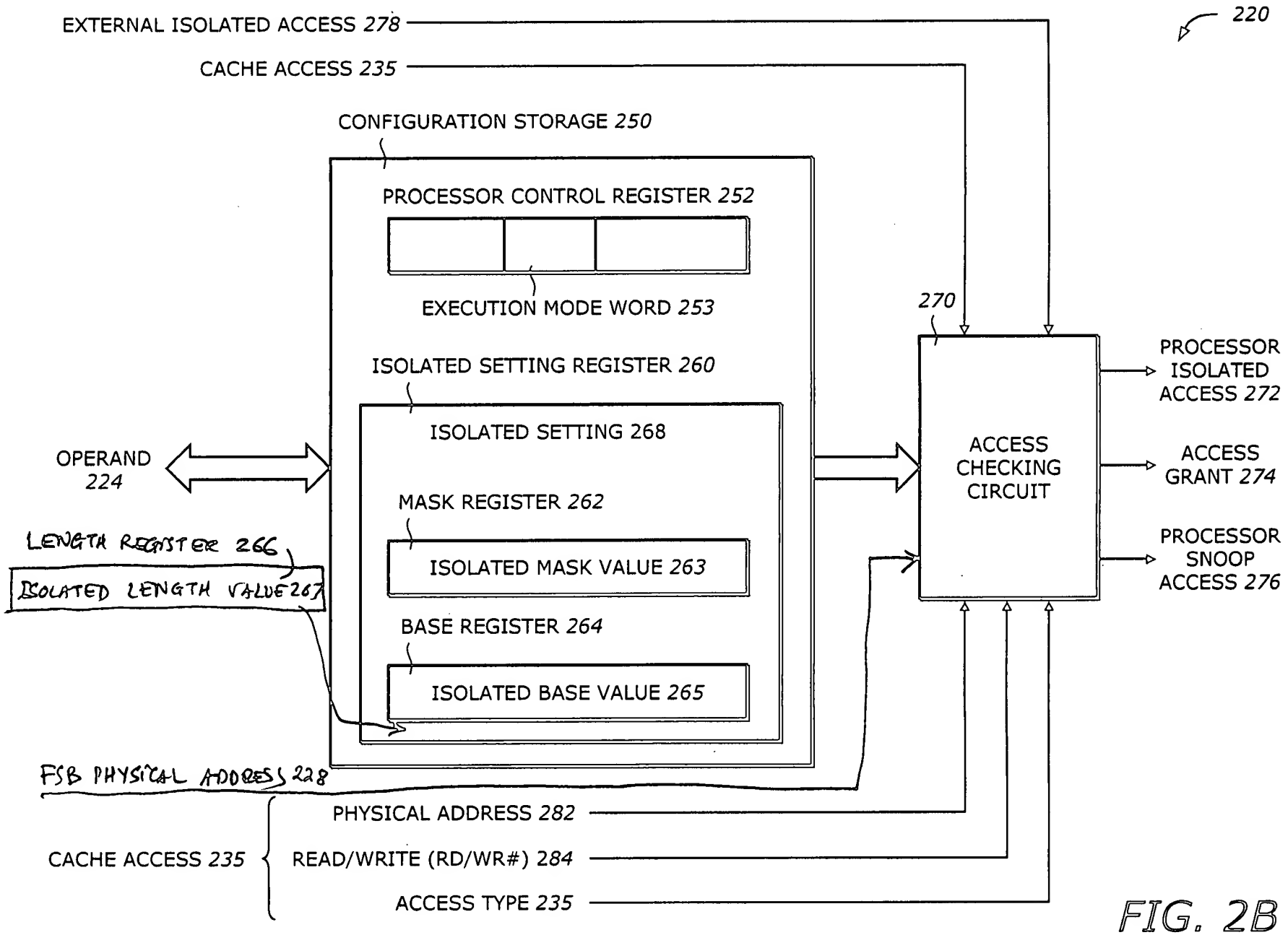
220
EXTERNAL ISOLATED ACCESS 278
CACHE ACCESS 235
CONFIGURATION STORAGE 250
PROCESSOR CONTROL REGISTER 252
EXECUTION MODE WORD 253
270
ISOLATED SETTING REGISTER 260
ISOLATED SETTING 268
OPERAND 224
MASK REGISTER 262
ISOLATED MASK VALUE 263
LENGTH REGISTER 266
ISOLATED LENGTH VALUE 267
BASE REGISTER 264
ISOLATED BASE VALUE 265
ACCESS CHECKING CIRCUIT
PROCESSOR ISOLATED ACCESS 272
ACCESS GRANT 274
PROCESSOR SNOOP ACCESS 276
FSB PHYSICAL ADDRESS 228
PHYSICAL ADDRESS 282
CACHE ACCESS 235
READ/WRITE (RD/WR#) 284
ACCESS TYPE 235

FIG. 2B

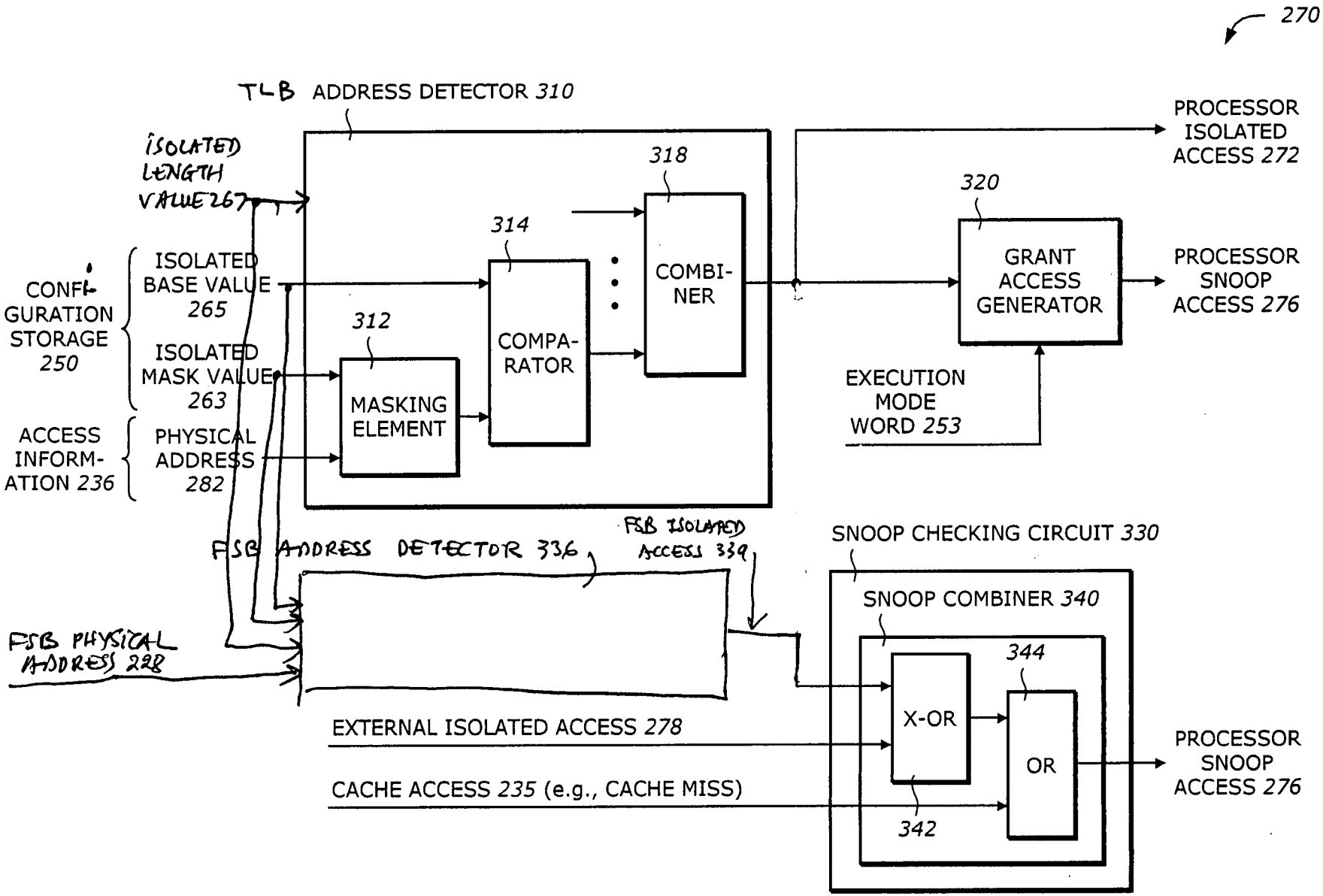
270
TLB ADDRESS DETECTOR 310
ISOLATED LENGTH VALUE 267
CONFIGURATION STORAGE 250
ISOLATED BASE VALUE 265
ISOLATED MASK VALUE 263
ACCESS INFORMATION 236
PHYSICAL ADDRESS 282
312
MASKING ELEMENT
314
COMPARATOR
318
COMBINER
320
GRANT ACCESS GENERATOR
PROCESSOR ISOLATED ACCESS 272
PROCESSOR SNOOP ACCESS 276
EXECUTION MODE WORD 253
FSB ADDRESS DETECTOR 336
FSB ISOLATED ACCESS 339
SNOOP CHECKING CIRCUIT 330
SNOOP COMBINER 340
344
X-OR
OR
342
FSB PHYSICAL ADDRESS 228
EXTERNAL ISOLATED ACCESS 278
CACHE ACCESS 235 (e.g., CACHE MISS)
PROCESSOR SNOOP ACCESS 276

FIG. 3A

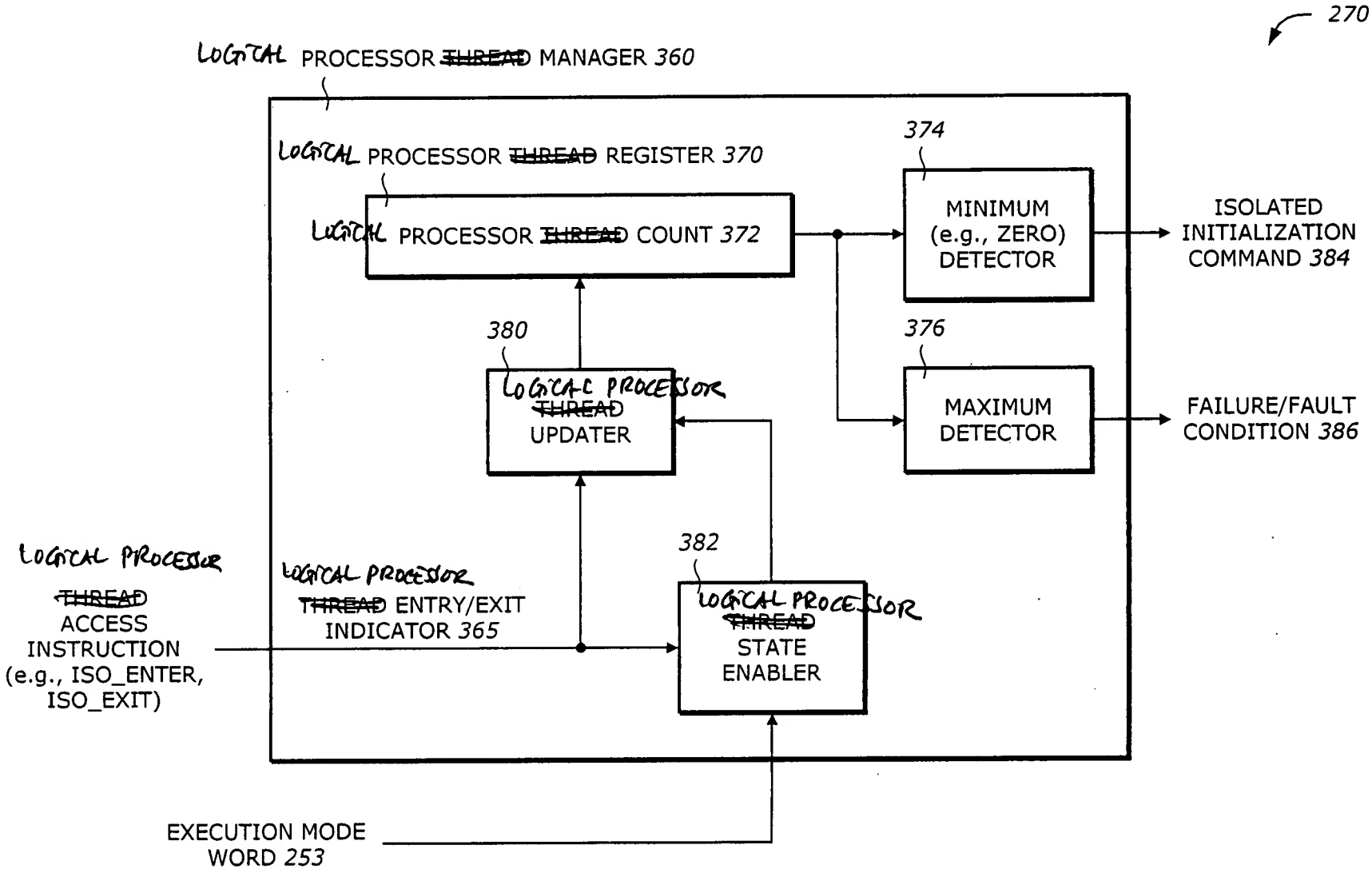
270
LOGICAL PROCESSOR ~~THREAD~~ MANAGER 360
LOGICAL PROCESSOR ~~THREAD~~ REGISTER 370
LOGICAL PROCESSOR ~~THREAD~~ COUNT 372
374
MINIMUM (e.g., ZERO) DETECTOR
ISOLATED INITIALIZATION COMMAND 384
380
LOGICAL PROCESSOR ~~THREAD~~ UPDATER
376
MAXIMUM DETECTOR
FAILURE/FAULT CONDITION 386
LOGICAL PROCESSOR ~~THREAD~~ ACCESS INSTRUCTION (e.g., ISO_ENTER, ISO_EXIT)
LOGICAL PROCESSOR ~~THREAD~~ ENTRY/EXIT INDICATOR 365
382
LOGICAL PROCESSOR ~~THREAD~~ STATE ENABLER
EXECUTION MODE WORD 253

FIG. 3B

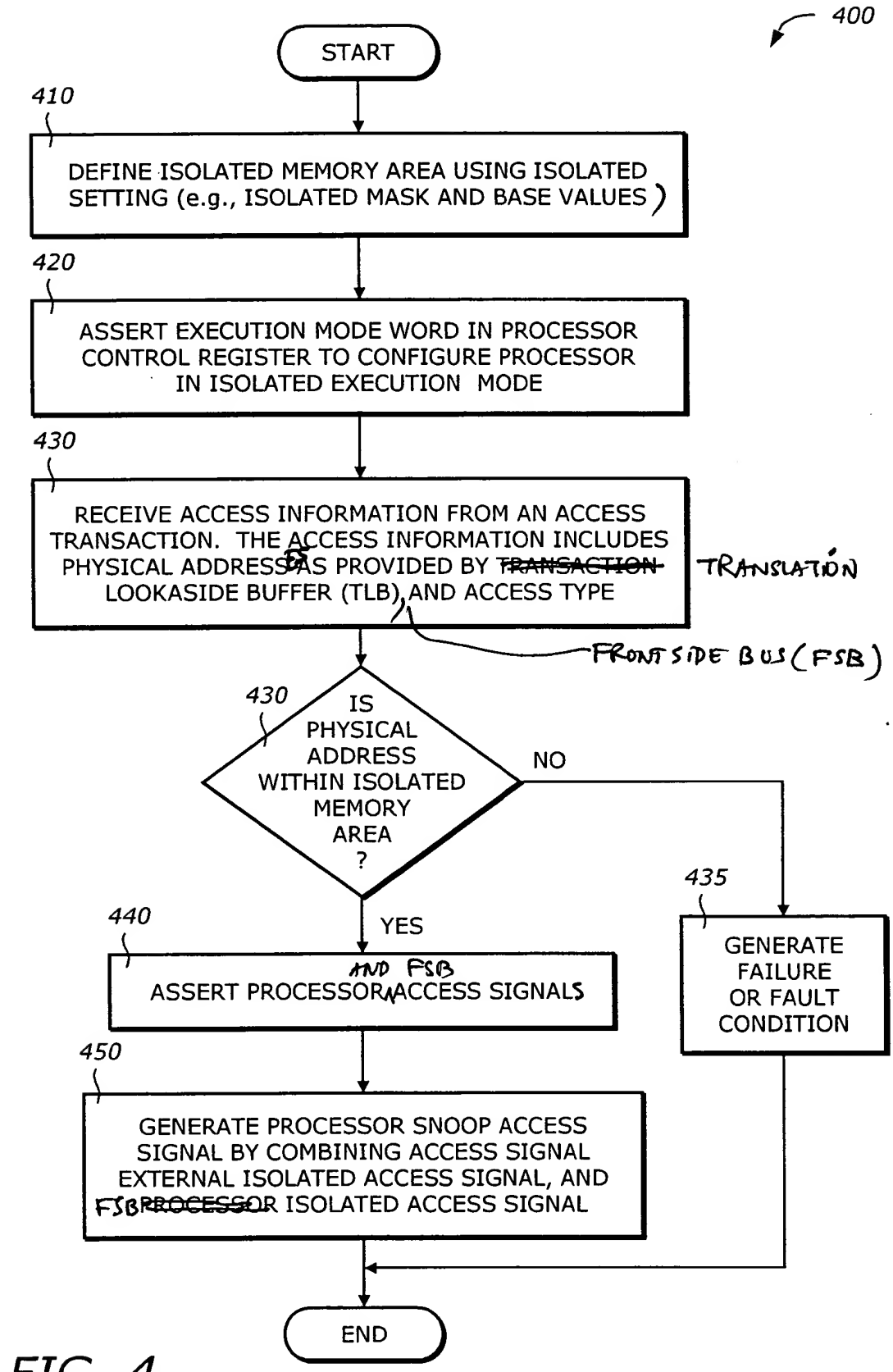
400
START
410
DEFINE ISOLATED MEMORY AREA USING ISOLATED SETTING (e.g., ISOLATED MASK AND BASE VALUES)
420
ASSERT EXECUTION MODE WORD IN PROCESSOR CONTROL REGISTER TO CONFIGURE PROCESSOR IN ISOLATED EXECUTION MODE
430
RECEIVE ACCESS INFORMATION FROM AN ACCESS TRANSACTION. THE ACCESS INFORMATION INCLUDES PHYSICAL ADDRESS AS PROVIDED BY ~~TRANSACTION~~ LOOKASIDE BUFFER (TLB), AND ACCESS TYPE
TRANSLATION
FRONTSIDE BUS (FSB)
430
IS PHYSICAL ADDRESS WITHIN ISOLATED MEMORY AREA ?
NO
YES
435
GENERATE FAILURE OR FAULT CONDITION
440
AND FSB
ASSERT PROCESSOR ACCESS SIGNALS
450
GENERATE PROCESSOR SNOOP ACCESS SIGNAL BY COMBINING ACCESS SIGNAL EXTERNAL ISOLATED ACCESS SIGNAL, AND ~~FSB PROCESSOR~~ ISOLATED ACCESS SIGNAL
END

FIG. 4

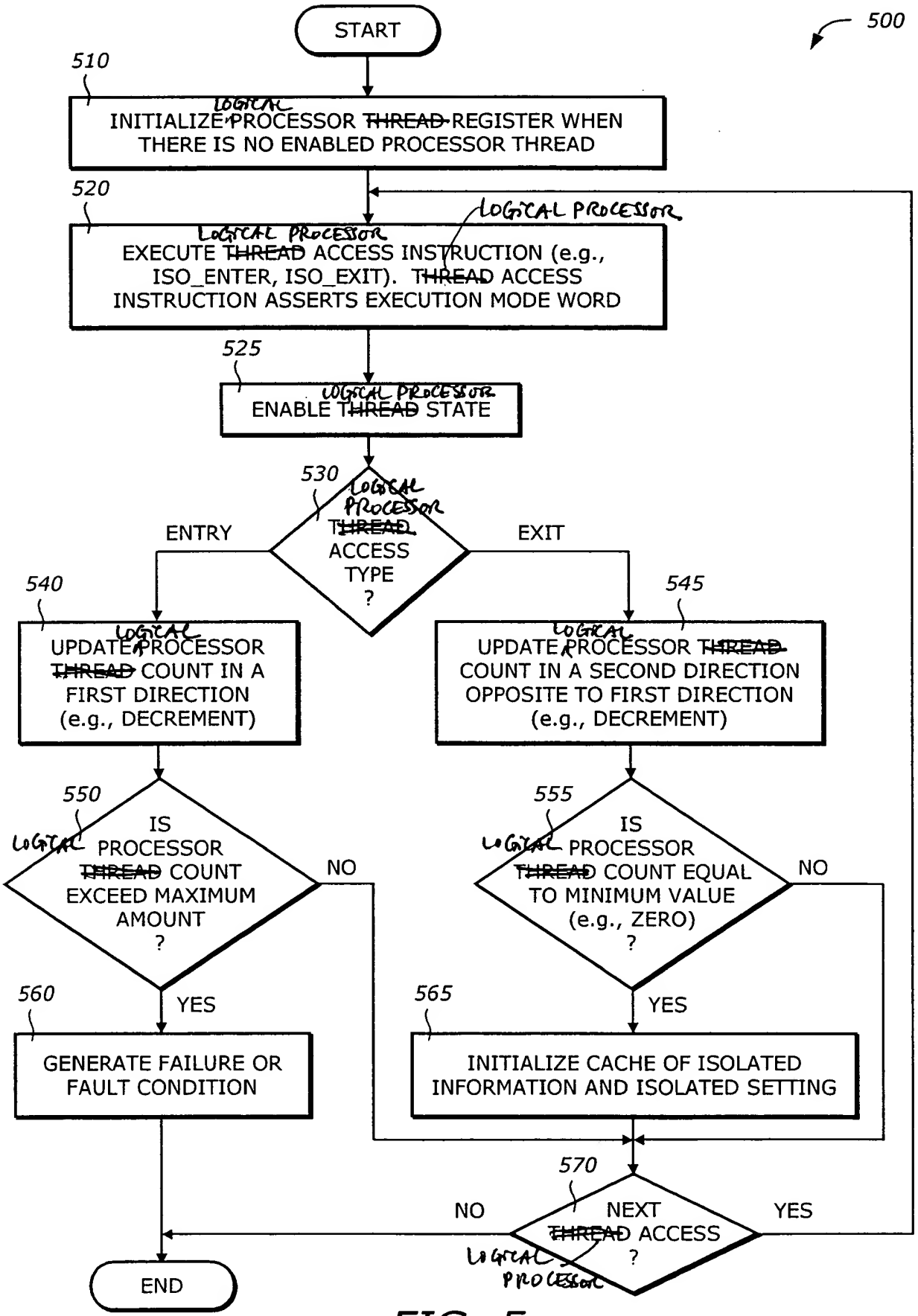
500
START
510
INITIALIZE LOGICAL PROCESSOR ~~THREAD~~ REGISTER WHEN THERE IS NO ENABLED PROCESSOR THREAD
520
LOGICAL PROCESSOR
EXECUTE ~~THREAD~~ ACCESS INSTRUCTION (e.g., ISO_ENTER, ISO_EXIT). ~~THREAD~~ ACCESS INSTRUCTION ASSERTS EXECUTION MODE WORD
525
LOGICAL PROCESSOR
ENABLE ~~THREAD~~ STATE
530
LOGICAL PROCESSOR ~~THREAD~~ ACCESS TYPE ?
ENTRY
EXIT
540
LOGICAL PROCESSOR ~~THREAD~~ COUNT IN A FIRST DIRECTION (e.g., DECREMENT)
545
LOGICAL PROCESSOR ~~THREAD~~ COUNT IN A SECOND DIRECTION OPPOSITE TO FIRST DIRECTION (e.g., DECREMENT)
550
LOGICAL PROCESSOR ~~THREAD~~ COUNT EXCEED MAXIMUM AMOUNT ?
NO
YES
555
LOGICAL PROCESSOR ~~THREAD~~ COUNT EQUAL TO MINIMUM VALUE (e.g., ZERO) ?
NO
YES
560
GENERATE FAILURE OR FAULT CONDITION
565
INITIALIZE CACHE OF ISOLATED INFORMATION AND ISOLATED SETTING
570
NEXT ~~THREAD~~ ACCESS LOGICAL PROCESSOR ?
NO
YES
END

FIG. 5